Social Security Scotland
Tèarainteachd Shòisealta Alba

Data Protection Assurance Framework Overview

04 May 2020

Background

1. The Data Protection Act 2018 (the 'Act') and General Data Protection Regulations (GDPR) set out mandatory obligations for organisations processing personal data. The penalty for non-compliance is significant and can result in a fine of up to €20 million.

2. GDPR introduced an accountability principle which requires appropriate measures, procedures and records in place to demonstrate, at any point in time, our compliance with the legislation. In response Social Security Scotland's Data Protection and Information Governance Team have developed a Data Protection Assurance Framework.

Framework

4. Assurance can be described as confidence, based on sufficient evidence, that internal controls are in place, operating effectively and objectives are being achieved.

5. The Data Protection Assurance Framework has been designed to assess compliance with legislation and foster a culture of continuous improvement for Data Protection.

6. The framework has four elements:

- A set of assessable requirements for the Agency
- Health Check assessments, tailored for individual Divisions and Units, to assess compliance and effectiveness of controls both locally and organisationally.
- Regular gathering and assessment of reliable Management Information for key indicators of data protection and assurance measures to assess performance and indicate trends.
- Evidence based reporting through the Agency governance chain.

Data Protection Requirements

6. Underpinning the framework are a set of statutory, mandatory and best practice Data Protection requirements for organisations such as Social Security Scotland to ensure compliance. 102 requirements have been identified which are organised in 11 categories set out in Annex A.

7. Evidence against the requirements will be gathered and assessed to determine the Agency's compliance position. This will allow performance and effectiveness to be

assessed providing an opportunity to make recommendations for continual improvement in each area to strengthen our overall position.

Data Protection Health Checks

8. Data Protection Health Checks will be conducted by the Data Protection team with business units to gather evidence and assess effectiveness and compliance. Health Checks will be tailored to the relevant business area. The team will adopt a risk-based approach to prioritise and schedule health checks in consultation with the Agency Data Protection Officer and Senior Management.

6 Health Checks will be a formal, collaborative process with business units incorporating:

- a scoping meeting
- an agreed Terms of Reference
- an evidence questionnaire
- fieldwork
- assessment
- a report to management including tailored recommendations for agreement and acceptance
- a follow-up review of progress with recommendations

Management Information

7 Management Information will be gathered or generated in respect of key data protection indicators for Social Security Scotland. The information will be collated and presented in a performance dashboard.

8 Reporting of the dashboard will be structured and will include or inform:

- Monthly updates for the Data Protection Officer
- Quarterly updates for the Agency Leadership Team
- An assurance statement for the Agency Corporate Assurance Framework
- Evidence for an annual report to the Executive Team

Reporting

8 As set out in Annex B the Agency Data Protection Officer will receive regular, at least monthly, updates and reports on findings and progress. Reports of completed Health Checks will be provided to the management of the relevant Division or Business Unit. The Data Protection Assurance Framework will provide evidence for the Corporate Assurance

Framework. An annual report will also be produced for the Executive Team based on evidence from the Data Protection Health Checks and Performance Monitoring.

9. Ad-hoc reports will be produced to escalate findings of significant concern or emerging risk to the Audit and Assurance Committee or Executive Team as appropriate with associated action plans or recommendations.

[Redacted]
Senior Data Protection Practitioner

Social Security Scotland
Tèarainteachd Shòisealta Alba

ANNEX A

Categories of Data Protection Requirements

Category	Count	Evidence Sources (in addition to Data Protection Officer review)
Data Protection Policy *adequate policies are in place covering key obligations with regular review and update*	4	Data Protection Team Internal/External Audit
Governance *accountability, expertise and resources are in place with suitable governance structures*	12	Health Check reviews Internal/External Audit
Supporting Policies and Guidance *complimentary HR, Records Management and Security policies are in place and adequate*	5	Health Check reviews
Record of Processing Activities *compliant records of personal data processing are kept and maintained*	14	Health Check reviews Records Management Reviews
Privacy by Design *embedded in the culture of the organisation with effective processes and guidance*	6	Health Check reviews Data Privacy Impact Assessments
Information Security *effective physical and digital security measures are in place and monitored*	22	Cyber Security Team Information Risk Assessments Health Check reviews Internal/External Audit
Third Party Risk *management of partners, formal agreements and supply chain contracts and performance*	5	Health Check reviews Procurement Specialists
Training and Awareness *all staff and contractors including those with specific duties are adequately trained*	8	Health Check reviews Management Information Learning & Development Team
Data Subject Rights *individuals are made aware of their rights which are respected and supported*	16	Data Protection Team Information Rights Network Privacy Notice reviews
Personal Data Breaches *incidents are reported, investigated, managed and resolved with lessons learnt*	6	Incident Management Tool Management Information Health Check reviews
Self-Assessment effective review and continuous improvement	4	Health Check reviews Cyber Security Team Data Protection Impact Assessments
Total	102	

Social Security Scotland
Tèarainteachd Shòisealta Alba

Annex B

Data Protection Assurance Framework and Reporting Diagram